

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

WHITE PAPER

Identity and Access Management

“I AM Who I Say I AM”

Virginia’s Council On Technology Services
Identity and Access Workgroup

March 27, 2007

Workgroup Members: Dave Burhop, DMV CIO, Chair
Shirley Payne, UVA Director for Security
Coordination and Policy
Don Kendrick, VITA Senior Manager of
Security Operations
Lana Shelley, DMV Director of Systems
Development
Marie Greenberg, DMV Director of IT Security
Joanne Maxwell, DMV Director of Policy and
Legislative Services

Intity and Access Management

I AM Who I Say I AM

Contents:

Introduction

Regulatory Compliance

Successful Large Organizations

Best Practices

Available Technologies

Recommendations

Conclusion

Introduction

One of the most important issues facing us today is Identity and Access Management (IAM) and the technology we will select to authenticate citizens, government and business. Government agencies (federal, state and local) around the world are expanding their services and accessibility to each other, their employees, citizens, vendors and suppliers. Over the years, agencies have implemented a multitude of applications with incompatible platforms. This has resulted in inconsistent management of identities and ineffective auditing procedures. With the increased number of systems and users, this approach has become impractical, costly, and insecure. The risk of identity theft, unauthorized access and failure to meet regulatory compliance has increased. "Silos" have emerged with the increased access to information, which has resulted in duplication of efforts resulting in an even greater challenge of managing these users and identities. As Intranet, extranet and Internet access has evolved, security has become an even larger issue. The opposing policies of protecting citizen privacy and freedom on one side and protecting national security and the laws of the land on the other has resulted in inconsistent processes, rules and laws. We must balance our need for easy access to information with the requirement for identity protection. Effectively managing security begins with identity and access, knowing and controlling who is accessing your system and monitoring what they have done.

Background

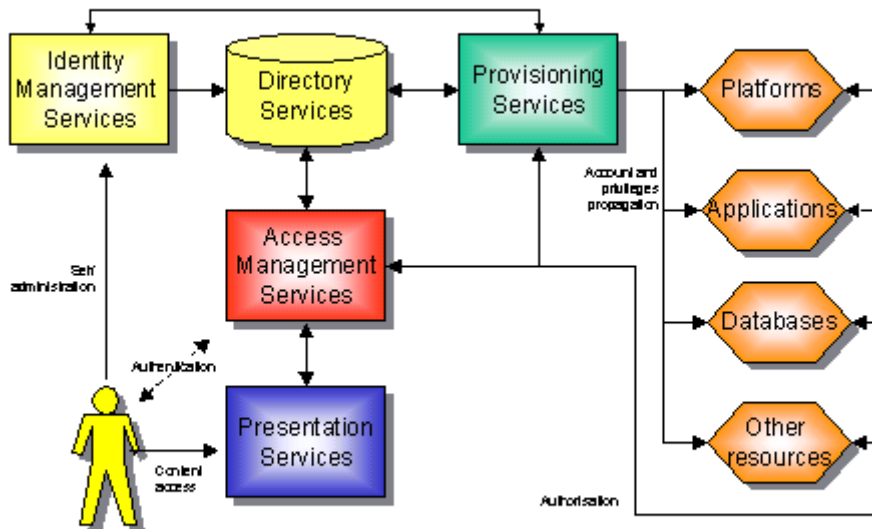
Users are required to remember upwards of 15 passwords (where do you have yours written down?) for various systems, having to manage multiple user identities and passwords for network access, email, and web access. According

to a recent survey, about 74% of IT personnel in the industry said their users must remember too many passwords, and 63% said coping with multiple password policies is a significant problem. Identifying themselves throughout the day is not only annoying to the user but can lead to security breaches as users circumvent security policies. RSA Security, Inc. says that according to industry analysts, it is estimated that as much as 40% of help desk calls are password-related and that the cost is between \$20 to \$50 per reset. More than 56% said they're handling too many password resets.

What is Identity & Access Management?

There are multiple variations of IAM, but the most common definition includes identification & authentication, password management, role management, single sign-on, access management, and auditing. Identity management is the capability to manage all user accounts and profiles across the IT environment via user roles and business rules. Access management is the ability to manage access control policies across multiple platforms. An integral part of identity management is to ensure that users have secure, convenient access to the resources needed (and only the resources needed) to perform their work. By using the process of authentication, authorization and auditing, access management becomes the key to a successful IAM program. Access management is often referred to as the gold standard because of the symbol "AU" from the first two letters of all three processes.

-An overview of Identity and Access Management is as follows:



- Directory service provides a central identity repository and reconciliation of identity details between application specific directories.
- Identity management service provides tools to manage identity details stored in the directory.
- Access management services implement authentication of web based users and enforces access control over the web-based transactions.
- Provisioning service covers centralized user administration capabilities and serves mainly for propagation of user account changes and access rights across individual back-end applications. In this manner it is bridging the gap between e-business systems and enterprise applications security.
- Presentation service is providing a personalized interface for all user interactions with the system.

Regulatory Compliance

The list of regulations regarding security, privacy and audit functions is growing in every country and industry. Many CIOs rank regulatory compliance among their top concerns. What these laws have in common is the requirement that agencies be able to account for how, what, by whom and when their information is being accessed as well as assuring individual privacy is not compromised.

Some of the relevant regulatory guidance governing IAM are:

- Health Information Portability and Accountability Act (HIPAA): applies privacy and security standards to protect patient identities and sensitive health and treatment information.
- Gramm-Leach-Bliley (GLB): applies to financial services firms operating in the U.S. and is designed to protect consumers' financial information from unauthorized access.
- Homeland Security Presidential Directive-12 (HSPD-12): sets the policy for a common identification standard for Federal employees and contractors. Although written for the federal agencies, state and local governments with federal grants must work within these requirements.
- Privacy Act of 1974: mandates that each agency has in place an administrative and physical security system to prevent the unauthorized release of personal records. It was amended in 1988 to include records used in automated programs.
- Family Educational Rights and Privacy Act (FERPA): Generally, schools must have written permission from the parent (of a minor) or eligible student to release information from a student's education record.
- Executive Order of Critical Infrastructure Protection: to ensure protection of information systems for critical infrastructure, including emergency

preparedness communications and the physical assets that support such systems.

- Federal Information Security Management Act (FISMA): imposes a mandatory set of processes that must be followed for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency.
- Bank Secrecy Act: requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding \$10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.

Successful Large Organizations – what they are doing to ensure you are who you say you are.

Government Initiatives

Border and travel initiatives using biometrics-based security are prompted by a belief that this will reduce terrorism, but this is unclear if it will work. Several countries are in various implementation stages of national ID initiatives. The Real ID Act is forcing a distributed, state-by-state, national ID standard for interoperability, as each state must be able to verify all other states ID issuance. This may result in states creating a central identity agency (independent agency?, DMV?, other agency?) to authenticate and register its citizens. However, a major concern is the costs of conversion. HSPD-12 is pushing for deploying a multi-technology smart card for logical and physical access, to be carried by all federal employees.

As government agencies, we want to use the 24/7 availability of the web to provide customers with around-the-clock access to information. This includes the ability to process transactions. However, we are concerned with identity theft, security of personal data, financial and confidential data as well. We need to provide auditable proof that only appropriate access is granted to critical data.

At the state and federal level, Identity & Access Management is being actively researched and in many cases is already in place. Nebraska, New York, Massachusetts, Iowa and other state governments have already implemented IAM standards and guidelines and are actively pursuing compliance with HSPD-12 and other regulatory guidance.

-In March of 2005, Nebraska implemented a standard to provide an enterprise solution for IAM. Their objective was to build an identity-based portal to integrate disparate applications, enable secure web access to applications and data, and enable users to access applications from their office or remote locations.

Another goal was to ensure a solution that is scalable to meet the future needs of the state, their clients and business partners. Their proposed method incorporated User ID & password, two-factor authentication and X.509 certificates.

-In January of 2007, New York State implemented The Identity and Access Trust Model, which is applicable to all systems, and networks owned and operated by state entities and other New York State government agencies. Their process is a structured approach to design and implementation using common, shared processes and technologies.

-The Commonwealth of Massachusetts is developing a centrally supported identity service to support different levels of single sign-on. Massachusetts's portal's centrally supported identity service requires state employees to use two different electronic identities. One for each role, that of state employee and that of private citizen so as to reduce abuses in the arena of privacy and fair information practices.

-The Commonwealth of Pennsylvania has launched an enterprise-wide effort addressing identity protection and access management (IPAM) comprised of a dedicated governance structure, advisory board and technical architecture team using the standards and practices of:

- Enterprise Directory Services
- Access Management and Control
- Federation
- Public Key Infrastructure

-Iowa has begun an innovative Identity-Security Project to create a clearinghouse where documents used to create identity (birth certificate, death certificate, driver's license, marriage license and SSN) can be linked. This clearinghouse will allow agencies to track identity theft as well as cross-link identity verification.

-The University of Texas Health Science Center at Houston (UTHSC-H) is a national leader in the implementation of middleware infrastructure. They function as an identity provider issuing individuals with digital credentials at the "Medium level of assurance." They use a single UTHSC-H username/password and two-factor authentication based on digital IDs (i.e. private/public key pairs) contained in USB tokens.

-On the federal side, Anteon has integrated a flexible solution to meet the guidelines of HSPD-12 and Federal Information Processing Standard Publication 201 (FIPS-201) PIV requirements for several federal agencies. They have implemented solutions on major identity management programs such as the Department of Defense (DoD) Common Access Card (CAC) 'Smart Card' Program, the U.S. National Guard Physical Access System, the U.S. Department

of Homeland Security, U.S. Department of State and the Transportation Worker Identification Credential (TWIC) program.

The U.S. General Services Administration (GSA) has certified Novell's identity assurance solution for HSPD-12. Novell's identity assurance solution includes identity management technologies to provide seamless integration with single-sign on and access policies. These are used to govern both physical and logical access to government facilities and resources as well as the ability to centrally provide real time monitoring of PIV card activity.

The Department of the Army is in the process of converting its' "separate login & password for each system and network" to a single-sign-on using the Army Knowledge Online web interface.

The Department of Defense has implemented "Secure ID" procedures in varying degrees across the Departments of the Navy & Marine Corps, Army and Air Force. In 1999, the Navy initiated PKI using "soft certificates" for identification and encryption. In 2001, the DOD began issuing these certificates using the Common Access Card (CAC). This program is now well integrated into the various services and is used for identification, access and services for all military members and federal employees. The CAC ID card is issued to all US Service personnel and contractors on US Military sites. This card contains biometric data and digitized photographs. It also has laser-etched photographs and holograms to add security and reduce the risk of falsification. There have been over 10 million of these cards issued.

- Since 9/11, the Virginia Department of Motor Vehicles (DMV) has strengthened issuance processes for driver's licenses and identification cards. Some of the changes were the result of administrative action, while others were dictated by legislation.

A key component of these changes involved enhancement of existing, or implementation of new, requirements pertaining to proof of identity, Virginia residency, legal presence and SSNs. After an extensive study of various documents, DMV identified those documents that appeared to be the most reliable for proving each of these elements and established a list of documents that could be accepted as proof of identity, Virginia residency, legal presence and SSN. DMV has also subscribed to electronic systems offered by the federal government for verifying SSNs and legal presence of non-citizens.

As DMV's driver's license and ID card issuance process was enhanced, the process and/or the credentials issued began to gather the attention of legislators and other state agencies seeking to rely on those processes and credentials for proof of identity, SSN or legal presence.

For instance:

- As a result of legislation imposing very specific proof of legal presence requirements for issuance of driver's licenses, DMV was probably the first entity in the Commonwealth to develop and vet with entities such as United States Customs and Immigration Services and the American Immigration Lawyers Association, a comprehensive list of acceptable documents for proof of legal presence. Subsequently, the DMV list became the defacto/default list when legal presence was being considered as a prerequisite in other situations. For instance, the DMV list was specifically identified as the acceptable document list in a bill mandating that all agencies of the Commonwealth verify the lawful presence of any person who, for any purpose, must establish that they are a legal resident in Virginia (See SB521, 2004).
- During the 2005 session of the General Assembly, legislation was enacted (See HB1798/SB1143) that requires proof of legal presence for receipt of public benefits and the resulting law specifies that acceptable proof is the same documentary evidence that is required for issuance of driver's licenses. At various points in time, the language contained in SB1143 or proposed amendments would have established driver's licenses as indicia of legal presence and would have required DMV to promulgate regulations for all state agencies to implement and enforce the proof of legal presence requirement.
- The Smartcard ID Working Group and Commonwealth Credentialing Task Force were recently established in the Commonwealth. It appears that the primary objective of these groups, consisting of representatives from various Virginia state agencies, is to review, for purposes of security, the standardization of identification and credentialing for Virginia's first responders as well as state government agencies and employees. Upon completion of any review, these entities are to propose and coordinate the approach that the Commonwealth should take in issuing identification cards and other credentials for various purposes.
- Recently, as a result of the Deficit Reduction Act of 2005 (DRA), which mandates new citizenship and identity verification requirements for Medicaid recipients, the Department of Medical Assistance Services has called upon DMV to assist the agency in fulfilling its new identity and citizenship authentication/verification role. The DRA was discussed at the International Conference conducted by the American Association of Motor Vehicle Administrators in August of 2006 and was cited as the impetus that may drive many states to establish a single entity that performs authentication and identity management/verification for all agencies.

Under the REAL ID Act, issuance requirements for compliant credentials will be even more stringent than the requirements currently in place today for issuance of Virginia driver's licenses and ID cards. Ultimately, the issuance process will require not only presentation, but verification with the issuing entity, of acceptable documents for proof of identity, residency, address, legal presence and SSN. It is anticipated that this particular aspect of the REAL ID Act will be one of the more labor-intensive requirements of the Act. Currently, it requires approximately 37 FTEs at a cost of approximately \$ 2.1 million¹ annually for DMV to perform authentication of proof documents. At this point in time, it is estimated that for purposes of implementing REAL ID, DMV will need an additional 111 FTEs, at an estimated cost of \$ 4.6 million. These additional FTEs will be dedicated to performing authentication and verification of proof documents. Although the effective date for implementation of the Act is May, 2008 (draft regulations may grant 19 month extensions), various bills have already been introduced in Congress that would mandate particular uses for, or require additional information to be placed on, compliant credentials. Thus, it has become apparent that the reliance upon, and demand for, compliant credentials will be high.

Business and Technology Trends

There are various ways for organizations to provide strong security and user convenience.

- Biometrics are automated methods of recognizing a person based on a physiological characteristic or personal trait. Among the features considered measurable are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links

¹ Current staffing and associated costs include staffing in the CSCs as well as the Identification Review Services workcenter—which addresses exceptions and complex cases.

the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and cost effective. Imagine how this technology could significantly reduce or eventually eliminate the billions of duplicate customer records in databases across the world.

- Microsoft has promoted one response; namely the centralized identification model called .NET Passport. While this technology is in use, all user data is stored in one place prompting criticism by many in the industry for being a high security risk.

- The Liberty Alliance is a coalition of more than 170 businesses and organizations worldwide. General Motors (GM) was one of the founding members of Liberty. Liberty is considering the use of a Federated Identity as a corporate initiative to make their system easier, seamless, secure and private. Federated identity enables organizations to share trusted identities across the boundaries of the corporate network to remote offices, business partners and autonomous business units. GM sees digital identities as a keystone for the future, especially in ventures such as OnStar.

- AOL however, took a different approach. They focused on the issue of identity-based Web services, using the Liberty Alliance protocols for authentication and discovery services. AOL worked with a number of electronics device vendors who built Liberty layers into their products. AOL's vision for the future requires robust standards focused on privacy and security to implement devices that will communicate with applications on behalf of users. Many in industry believe that federated identification and Web-based identity management will become standard operating procedure.

Best Practices

- SPIDeR (Systems Partnering in a Demographic Repository), developed in 2005 by the Virginia Department of Social Services, performs as a single sign-on into various state and local systems to form a virtual real-time data warehouse. Inquiries tie a client's various records together via a common identifier while maintaining information on the data's source. This has eliminated thousands of staff hours logging into different systems (in some cases manually contacting the source agency) to prepare client profiles.

- MyVirginiaPin, developed as a Commonwealth project by Virginia DMV in 2001, was created as a single, secure key (PIN) to safely conduct government transactions on the Internet. The plan was to allow Virginia citizens to file tax returns, renew driver's licenses, view and order college transcripts and review unemployment or government assistance benefits. The objective was to give citizens a single, secure number to access Web-based services offered by state

agencies, local governments and educational institutions and was created to facilitate secure e-government transactions. Combined with Secure Sockets Layer (SSL) technology, MyVirginiaPin was designed to protect citizens' privacy and ensure the utmost security when conducting Internet transactions. Though the MyVirginiaPin application was successfully developed and tested, it was never implemented. The drawbacks of the system were:

- lack of support from upper levels of government
- lack of advanced technology (especially voice recognition for access to services) at some agencies
- lack of standard IT Architecture and Infrastructure for interoperability
- no statewide oversight
- little agency collaboration
- many applicants were not in the DMV database
- did not accommodate business PINs.

With support from the upper levels of government and all government agencies, MyVirginiaPin can be a framework from which to launch a statewide IAM program. Today, six years later, the VITA/NG Partnership has the technology and conceptual design to implement a Federated or Enterprise program, which will encompass state employees, businesses, vendors and private citizens. With the completion of the new data centers, consolidation of the mainframe, extranet, intranets, LANs, and Web services, this creates the infrastructure to position us for an enterprise solution. The virtual one-stop shopping originally envisioned in the MyVirginiaPin concept is a viable option.

-New York has implemented the Identity and Access Management Trust Model. This is largely based on the E-Authentication Guidance for Federal Agencies (issued by the OMB) and NIST 800-63 Recommendation for Electronic Authentication. The draft Trust Model establishes four Trust Levels, which provide a progressively higher level of confidence that the individual is who he or she claims to be. The Trust Model establishes a standard set of processes, which include:

- registering or identifying users,
- issuing credentials,
- using the credential, and
- record keeping and auditing.

New York State envisions their program “to extend across the state enterprise connecting to all levels of government, business partners and the public and will improve security, interoperability, and efficiency.”

-CA's eTrust Identity & Access Management Suite provides the infrastructure to comply with HSPD-12. Their solution covers enterprise, extranet and mainframe access and consists of:

- Authentication- uses multiple authentication standards and supports federated identity through SAML and Liberty Alliance
- Policy enforcement using access control
- Extranet management that secures web content, regulates web access and provides single sign-on across internal and external websites. This scales to millions of users, reducing the complexity of managing multiple web applications with centralized policy management
- Single sign-on
- Web services security
- Auditing
- Directory-independent infrastructure
- Mainframe Environment support

-The Department of Homeland Security (DHS) has partnered with General Dynamics to implement the First Responder Authentication Credentials (FRAC). General Dynamics Information Technology supported the Department of Homeland Security (DHS) Office of National Capitol Region Coordination (NCRC) disaster preparedness Demonstration Winter Storm by providing First Responder Authentication Credential (FRAC) identity cards. The nationwide demonstration brought together federal, state and local first responders as well as the Department of Defense (DoD) and intelligence agencies to demonstrate in part, the use of the FRAC. The FRAC is an identity management system for emergency responders that creates a common, interoperable credential enabling first responders to quickly and easily access government buildings and incident areas in the event of a terrorist attack or other disaster. The cards, which are compliant with Federal Information Processing Standard 201 (FIPS 201), save significant time and help responders more effectively assist victims. General Dynamics provided its ChoiceID(TM) managed service solution, developed and delivered in cooperation with Lockheed Martin, for enrollment support and privilege hosting for the FRAC cards. More than 50 organizations in over 20 locations participated in Winter Storm. The General Dynamics and Lockheed Martin team issued cards to first responders in the Pennsylvania Region 13 Task Force in the Pittsburgh area, Southwest Texas Regional Advisory Council for Trauma Medicine (STRAC) in the San Antonio area, the Maryland Department of Transportation (MDOT), Maryland Department of Health and Mental Hygiene (MDHMH) and Maryland state police personnel.

-Arlington County, partnering with the Commonwealth of Virginia in the First Responder Partnership Initiative, is the first county in the nation to issue the new first responder credential. Arlington County is piloting the nations' first test of the FRAC and has issued over 1,400 cards to emergency services workers so far. The FRAC cards allow officials to electronically confirm the identity of first responders in the field. As a result, authorities can make decisions faster about whether to grant or deny access.

The Commonwealth of Virginia's Office of Commonwealth Preparedness (OCP), in coordination with the Department of Transportation and Department of Motor Vehicles, has formed the Commonwealth Credentialing Task Force (CCTF) which will create a state ID first responder card also using the federal standard FIPS 201.

Available Technologies

There are many authentication choices available for ease of use, scalability, and efficiency of deployment. Companies like HP, Imprivata, CA, Aladdin, BMC have developed enterprise systems that encompass both internal and external customers using a variety of tools such as:

- Certificate management solutions: allows encryption and authentication of users and applications through the use of public and private keys.
- USB tokens and smart cards: increase user convenience and lower costs by combining multiple credentials on one device
- Software tokens: can be used with handhelds such as Blackberries, Palms, wireless phones as well as workstations
- Hardware authenticators: enables secure network access from any location using "tokens", this would increase user mobility
- Zero-footprint mobile solutions: allows affordable two factor authentication for portable devices (PDAs, cell phones)

Recommendations

As Frederick Chong of Microsoft states, "An identity management solution should not be made up of isolated silos of security technologies, but rather, consist of well integrated technologies that address the spectrum of scenarios in each stage of the identity life cycle. Identity and Access Management is comprised of three indispensable elements: policies, processes and technologies. Policies refer to the constraints and standards that need to be followed in order to comply with regulations and business best practices; processes describe the sequences of steps that lead to the completion of business tasks or functions; technologies are the automated tools that help accomplish business goals more efficiently and accurately while meeting the constraints and guidelines specified in the policies."

Federation offers a form of single sign-on, but it is more than that. Federation implies a delegation of responsibilities honored through trust relationships between federated parties. Federated Identity Management (FIM) is an arrangement that can be made among multiple enterprises that enables subscribers to use the same identification data in order to obtain access to the

networks of all enterprises in the group. The use of such a system is sometimes called identity federation. Identity federation offers economic advantages, as well as convenience, to enterprises and their network subscribers. For example, multiple agencies can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust. Authorization messages among partners in a FIM system can be transmitted using Security Assertion Markup Language (SAML) or a similar Extended Markup Language (XML) standard that allows a user to log on once for affiliated but separate Web sites or networks. One of the key components of a federated approach would be to establish, perhaps under VITA governance, uniform system standards, technical standards, business processes and responsibilities. An identity management system should support common identity needs of governmental and private transactions, reduce costs, enhance service quality, safeguard the health and safety of the public and protect individual privacy.

Federation technology utilizes a trust model. There are several trust models, but the most common are:

- Hub-and-spoke – utilizes a central broker that is directly trusted by the federating parties.
- Hierarchical – two parties have an indirect trust relationship if they both have a trust path in their respective branches in the hierarchical tree to a common root authority.
- Peer-to-peer Web of Trust- a collection of ad-hoc direct trust relationships.

RSA Security's approach outlines an effective Identity & Access Management strategy. The goal is:

- One user with one identity in one infrastructure, single sign on (SSO).
- Implement a common infrastructure for the components of the IAM solution, to be centrally configured and managed.
- Next, replace the numerous online identities currently used by each user with one identity that is secure trusted and efficiently managed. With a single, common infrastructure we remove the inefficiencies and vulnerabilities of multiple architecture approaches. We will have the ability to define user rights in granular detail, in keeping with security policies and business goals, enforcing rights consistently across the enterprise, enhancing security and supporting compliance requirements. SSO makes it easier for users to practice good security. With only one password to remember, it is feasible to enforce a strong password and expect that users will not write it down.

To implement an enterprise solution for IAM, it would contain certain core components that:

- Provide user management with automated tools for updating user profile information in specific applications.
- Provide automated capabilities for activating user accounts and establishing access privileges across the entire enterprise.
- Allow an organization to assign and enforce user access right to diverse resources across Intranets, extranets, portals, and exchanges.
- Enhance trust in network, intranet, extranet and portal environments by requiring users to present conclusive proof of identity to be granted access to sensitive data and resources.

It is clear that there will continue to be increasing demand, at both the federal and state level, for authentication/verification of various types of personal information, such as identity, residency and legal presence, for official purposes. Legislative mandates, such as the DRA, are likely to continue and will require state agencies to implement, for the first time in their histories, policies and procedures to verify identity and other personal information of their clientele. It is also likely that ad-hoc groups tasked with addressing various identity and credentialing issues, such as the Smartcard ID Working Group/Commonwealth Credentialing Task Force, will be established from time to time. It appears the REAL ID Act's identification and verification requirements will be some of the most stringent that have ever been addressed by and implemented in the Commonwealth. In light of the foregoing, it is becoming clear that verification and management of identity are issues that are impacting multiple state agencies. If these issues continue to be addressed on an agency-by-agency or ad-hoc basis, there will be significant duplication of effort and resources, both human and financial, on the part of the Commonwealth as well as its citizens and residents.

The Commonwealth and its citizens and residents would stand to benefit from creating a centralized agency that performs authentication/verification functions for all other agencies. Under such a system, citizens and residents of the Commonwealth could have their personal information authenticated and verified in advance, before transacting business with any particular state agency. More importantly, such authentication and verification would need to be performed only once by a single agency, while other agencies could utilize and rely on the identity management services and database of the one authenticating/verifying agency for official purposes, such as determining eligibility for public benefits, issuing credentials, or issuing PINs.

Accordingly, it is recommended that the Commonwealth consider centralizing authentication and verification of identity, residency, legal presence, SSN and potentially other personal information for all agencies. If it is determined that it is in the best interest of the Commonwealth to centralize these functions, it will be

necessary to identify how best to accomplish centralization and to identify the entity or agency wherein centralization should be housed.

Conclusion

There is a multitude of viable solutions available. No solution is fail-safe or risk-proof. There is always a degree of risk involved. Security interdependency could lead to potential fraud between linked accounts. And of course, involving a third party always introduces risk. Whichever solution(s) is devised, it must allow agencies to minimize security breaches and quickly limit damages and financial or personal exposure.

Using the banking industry as a lesson, we can look at the history of the Automated Teller Machines (ATM). The advent of ATMs enhanced customer convenience on the one hand and created a problem on the other. How could customers remove cash from any ATM regardless of whether that ATM was sponsored by their bank? To resolve this, banks established ATM networks. They set common operating rules and regulations to ensure quality control and assurance. This allowed the banks to maintain security and mutual confidence.

The bottom line is that every agency in the state must be on the same page for this technology to work. Strong identification and verification measures must be implemented. There must be absolute faith in the identification of citizens to allow them access to state and federal services.

Strong authentication is one of the cornerstones of IAM. You must have a high degree of confidence in the identity of the users accessing your resources before you can allow them to move freely among multiple domains and systems. Equally important is to be able to trace a security breach back to its source. For this to work, agencies must have complete confidence that their partners are using ironclad authentication methods. We can no longer trust the password systems that people have been using for the last 20-plus years. They simply do not ensure that I am who I say I am.